The Trustworthy Computing Security Development Lifecycle

This paper discusses the Trustworthy Computing Security Development Lifecycle (or SDL), a process that Microsoft has adopted for the development of software that needs to withstand malicious attack. The process encompasses the addition of a series of security-focused activities and deliverables to each of the phases of Microsoft's software development process. These activities and deliverables include the development of threat models during software design, the use of static analysis code-scanning tools during implementation, and the conduct of code reviews and security testing during a focused "security push". Before software subject to the SDL can be released, it must undergo a Final Security Review by a team independent from its development group. When compared to software that has not been subject to the SDL, software that has undergone the SDL has experienced a significantly reduced rate of external discovery of security vulnerabilities. This paper describes the SDL and discusses experience with its implementation across Microsoft software. (19 printed pages)

Links

http://msdn.microsoft.com/en-us/library/ms995349.aspx
http://msdn.microsoft.com/en-us/library/ms995349.aspx